IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MINNESOTA

JAMF SOFTWARE, LLC, a limited liability company, Plaintiff, vs. PRAKASH MAHARAJ, an individual and KANDJI, INC., a corporation. Defendants.	Case No.

DECLARATION OF DINO MINUTOLO

NOW COMES Dino Minutolo who deposes and says:

1. I am over eighteen (18) years of age, legally competent to give this declaration, and have knowledge of the facts set forth herein.

Employment with Jamf and Qualifications

2. I serve as Senior Manager, Information Security ("InfoSec") at Jamf Software, LLC at Jamf's Global Headquarters located in Minneapolis, Minnesota.

3. In this role, I am responsible for managing Jamf's Security Operations ("SecOps") team. My job duties are:

a. Work with the Sales Organization including responding to all customer inquiries related to security and assisting in training sales teams on security related topics.

b. Provide tooling, dashboarding, and automation to all Security teams and supporting security tools as a service to other technical teams as needed.

c. Collaborate with other teams to solve security problems with minimal disruption to business functions.

d. Participate in investigations and troubleshooting of security issues to determine root cause and drive solutions.

e. Continuous improvement of policies, procedures, and technology.

f. Hire, train and assess performance of direct reports according to corporate policies and procedures.

g. Assist in the growth of employees through coaching, training, and career development activities.

h. Advises senior management on anticipation and prevention of potential threats, active exploits, and possible remediation.

i. Provides technical guidance to Product Management, Software Engineering, and Online Services during product/service planning, development, and operation.

j. Assists in the creation of corporate policies and procedures.

k. Develop and maintain security documentation and reporting.

l. Research new threats, risks, and attack vectors to Jamf infrastructure and software.

m. Performs security assessments on both internal and external resources/infrastructure.

n. Provide product expertise and counsel throughout the organization.

o. Performs other duties as required and completes all job functions as per departmental policies and procedures.

4. In addition to eleven years of professional experience in the fields of information security and cyber security, I earned the SEC-401 certification from SANS Institute and was also certified as a Microsoft Certified Systems Engineer.

Jamf's Salesforce Database

5. Jamf maintains unique, confidential, and proprietary information regarding its existing and prospective customers on Salesforce, a web-based data application ("Salesforce Database"). The information and materials maintained on the Salesforce Database are highly confidential.

6. Jamf also maintains other secure databases that contain confidential and proprietary information relating to customer preferences, pricing, sales performance, sales strategies and other highly sensitive business information.

7. Jamf's confidential information located in these databases are stored on servers within the United States.

8. Among the highly confidential and proprietary trade secrets on the Salesforce Database is:

a. Specific information regarding Jamf's go to market strategy for new and/or emerging markets such as India, the Middle East, and Africa, which includes unique pricing structures, different negotiated deals, and creative solutions for how to attract new business and compete with potential competitors in the market;

b. Target lists for prospective customers;

c. Details about existing customer agreements, including expiration and renewal dates, price points for renewals, rebates, market support, and confidential discussions regarding renewal strategy;

d. Details regarding contract proposals and quotes Jamf has offered and/or intends to offer to customers and prospective customers in various markets;

e. Confidential information regarding customers;

f. Confidential information regarding work-around issues with Jamf's products and services and test case documents;

g. Details about the progress of negotiations with existing customers for renewals and prospective customers for new business;

h. Pro formas modeling the financial aspects of a contemplated services agreement;

i. Information reflecting confidential discussions regarding the strategy for competing with incumbent service providers; and

j. An opportunities page with details about what various customers are looking to buy, product lists, sales stage history, and leads (new, current, or prospective customers).

9. Jamf takes substantial precautions to safeguard the confidential and proprietary trade secret information contained in its secured databases.

10. For example, its databases are user authenticated and IP address protected through Okta's single sign-on. Okta's single sign-on is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

Otka's single sign-on allows Jamf to have one set of password security standards across multiple different applications. This means that Jamf can set a high, consistent standard for password security because Jamf uses Okta to monitor and enforce those standards across all applications managed by Jamf.

11. Stated differently, it is accessible only by certain individuals, from certain electronic devices, and only from certain locations or IP addresses. Database authentication must also be changed every 90 days and users may not re-use their four most recent passwords. If a user attempts to reset their password, they must first respond to a security question they previously setup. If a user attempts to login from an unrecognized IP address, a notification is automatically sent to another device previously authorized by the user before the device is permitted access to Jamf's secure databases.

12. Additionally, a security token is required for accessing Jamf's secure databases via a third-party application for integration, such as Microsoft Excel or Outlook.

13. Access to Jamf's secure databases is limited to only those individuals who have a legitimate need for the information to effectively carry out their specific job duties.

14. Jamf also requires any individual to execute a confidentiality agreement before granting them access to Jamf's secure databases. Individuals are required to execute a Service Agreement that contains confidentiality provisions and a separate Non-Disclosure and Intellectual Property Assignment Agreement that also contains confidentiality provisions prior to being given authorization to access the secure databases.

15. Additionally, all contractors like Mr. Maharaj are required to attend and complete annual training titled "Protecting Our Data." Mr. Maharaj received this annual training on five separate occasions.

Investigation into Mr. Maharaj's Stealing of Jamf's Confidential and Trade Secrets Information

16. In my capacity as Senior Manager, InfoSec, I oversaw the SecOps team that performed the initial internal investigation of Mr. Maharaj's misappropriation of Jamf's confidential and trade secret information.

17. Once Jamf was aware that Mr. Maharaj might be joining a direct competitor, Jamf engaged SecOps to conduct an investigation.

18. SecOps utilized the monitoring function within Jamf Protect, one of its software products, to determine whether Mr. Maharaj unlawfully exported Jamf documents and information to a personal storage device and also whether he took screenshots of sensitive information.

19. The screenshots taken initially reported via Jamf Protect were among the screenshots seen being transferred to a personal USB device reported in Splunk and further correlated once a backup of the filesystem was provided by IT and investigated by SecOps. Splunk is a software tool used by the SecOps team to search, monitor, and analyze machine-generated data via a web-style interface. Jamf uses Splunk as a security incident event monitoring and investigation tool to centralize event logs across systems.

20. This part of the investigation showed that Mr. Maharaj had indeed taken 650 screenshots on his MacBook Pro 14, including some of Jamf's confidential and proprietary information stored on one or more of Jamf's secured databases in the weeks leading up to his departure from Jamf. Hundreds of these screenshots were determined to have been taken within the last few days of his tenure with the Company. A chart from InfoSec reflecting Mr. Maharaj's screenshot activity for the period in question is attached hereto as Exhibit 1.

21. The screenshots taken by Mr. Maharaj included, but are not limited, to:

a. Jamf's pricing information for customer(s) that Mr. Maharaj worked on for Jamf;

b. Jamf's report of customer names and value of their bookings for a particular Jamf market that Mr. Maharaj worked on for Jamf;

c. Jamf's August 2023 quotes for customer(s) showing pricing, volume, and channel discounts; and

d. Over 150 screenshots of Jamf's presentation for the Jamf 300 course.

22. SecOps' investigation also looked into USB activity as a potential method for how Mr. Maharaj could have stolen Jamf's confidential and trade secret information in conjunction with his departure from Jamf and new employment with Kandji.

23. The SecOps team investigated the USB activity by investigating logs from Jamf Protect for screenshots taken on the user's MacBook Pro 14, Splunk for file copy events, and a loading of the backup received by IT to confirm the contents of files by filename.

24. SecOps discovered that Mr. Maharaj created a folder on his Jamf-issued MacBook Pro 14 titled "Traisitioning [sic] Out of Jamf," moved Jamf's confidential and proprietary documents and information to the folder, and ultimately exported the documents and information to a personal USB device that he took with him to Kandji following his last day working for Jamf. SecOps determined Mr. Maharaj initially created the "Traisitioning [sic] Out of Jamf" folder on June 30, 2023.

25. In addition to the files exported from the "Traisitioning [sic] Out of Jamf" folder, Mr. Maharaj also exported files from his desktop to his personal USB device. Some of these files also included Jamf's confidential and proprietary documents, including customer lists and customer-specific presentations.

26. The severity and significance of Mr. Maharaj's actions was only heightened when SecOps discovered the scope of Mr. Maharaj's USB activity. SecOps's investigation revealed that in the weeks leading up to his departure from Jamf, Mr. Maharaj downloaded or copied

approximately 350,000 files to the personal USB device. Given the immense size of the exported data, SecOps believes Mr. Maharaj copied his entire drive to the personal USB device.

27. SecOps filtered the Splunk search to Mr. Maharaj's account as a local user. As a result, Jamf was able to confirm that Mr. Maharaj used his system credentials to log into his own MacBook Pro 14 (identified by known serial number QG7VFW1GPX) when the USB device was inserted to the MacBook and then the approximately 350,000 files exported to the USB device.

28. Mr. Maharaj's intentional misappropriation of Jamf proprietary information is further highlighted by the fact that numerous exported files in the "Traisitioning [sic] Out of Jamf" folder are titled as "screenshots," "pricing," or specific customer names.

29. The overwhelming majority of Mr. Maharaj's unlawful exportation of Jamf proprietary information took place after July 4, 2023.

30. Our investigation also showed that Mr. Maharaj took the Jamf 300 course, a Jamf certification course that provides users a deeper understanding of the macOs and iOS management capabilities within Jamf Pro. He took the course in the final days of his relationship with Jamf and weeks after he agreed to join Jamf competitor Kandji.

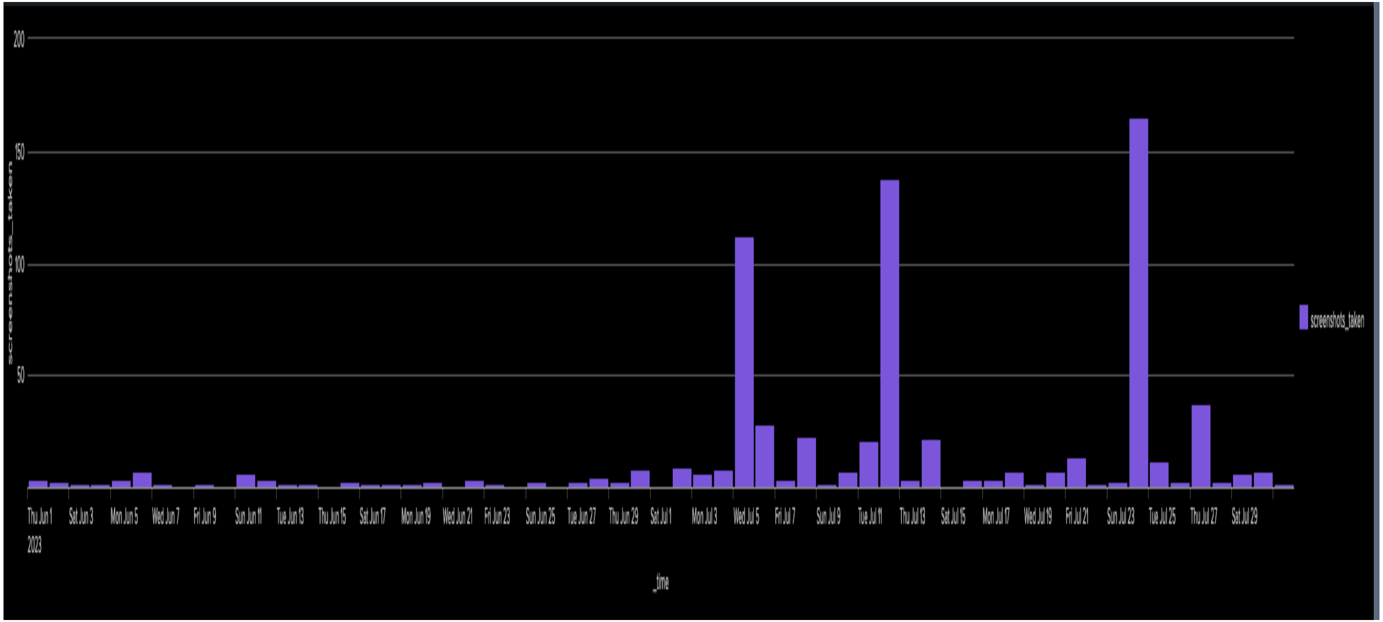
31. The Jamf 300 course has a written policy that expressly prohibits recording any part of the training and specifically bans sharing, copying, or reproducing images of training materials in any way. Despite this express prohibition, Mr. Maharaj took numerous screenshots of the Jamf 300 course programming. In fact, one of those screenshots is of the presentation page declaring that the course programming is confidential and proprietary to Jamf and recording is prohibited.

32. Based on our discovery that Mr. Maharaj appeared to be trying to misappropriate sensitive information, Jamf cut off Mr. Maharaj's access to Jamf's systems on July 27, 2023. After cutting off Mr. Maharaj's access, SecOps continued its investigation into the matter.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed this 17th day of August, 2023.

Dino Minutolo


200
150
100
50
screenshots_taken
screenshots_taken
Thu Jun 1
2023
Sat Jun 3
Mon Jun 5
Wed Jun 7
Fri Jun 9
Sun Jun 11
Tue Jun 13
Thu Jun 15
Sat Jun 17
Mon Jun 19
Wed Jun 21
Fri Jun 23
Sun Jun 25
Tue Jun 27
Thu Jun 29
Sat Jul 1
Mon Jul 3
Wed Jul 5
Fri Jul 7
Sun Jul 9
Tue Jul 11
Thu Jul 13
Sat Jul 15
Mon Jul 17
Wed Jul 19
Fri Jul 21
Sun Jul 23
Tue Jul 25
Thu Jul 27
Sat Jul 29
_time